Datenbank 11g R2: Die Kerberos-Unterstützung ist nun vollständig

Suvad Sahovic und Carsten Mützlitz, ORACLE Deutschland B.V. & Co. KG

Dieser Artikel beschreibt die wesentlichen Kerberos-Neuigkeiten, die mit der Datenbank-Version 11*g* R2 hinzugekommen sind.

In der letzten Ausgabe der DOAG News ist das Thema „Kerberos in der Datenbank-Welt“ detailliert beschrieben. Hauptthemen sind der Einsatz von Kerberos zur Authentisierung an Datenbank-Applikationen, der Einsatz von Microsoft Active Directory als Kerberos-Server sowie die Beschreibung der Funktionalitäten der Datenbank-Versionen 10*g* R2 und 11*g* R1. Wer hingegen eine starke Authentisierung von Kerberos mit der Oracle-Datenbank nutzen will, muss die Option „Advanced Security“ anwenden. Eine wesentliche neue Funktionalität, die nun in diesem Zusammenhang in 11*g* R2 mit der „Advanced Security“-Option eingeführt wurde, ist die Kombination unterschiedlicher Authentifizierungsarten beziehungsweise die Nutzung von Kerberos-Verfahren im „Delegation Modus“ (Constrained Delegation plus Protocol Transition).

Zuerst ist es wichtig, zwischen den beiden Authentifizierungs- und Autorisierungsmodellen „Trusted Subsystem“ und „Impersonation Modell“ zu unterscheiden. Beim „Trusted Subsystem“-Modell authentisiert sich der Endbenutzer gegenüber der Applikation1, anschließend baut diese mit der Datenbank eine Verbindung mit einem Proxy-User/DB-User/Schema-User auf und liefert die angeforderten Daten an den Enduser zurück (siehe Abbildung 1). Ergebnis ist, dass die Datenbank nicht weiß, wer die Daten angefordert hat. Das heißt, die Herausforderungen „Accounting“ und „Auditing“ sind von der Applikation1 zu lösen. Das läuft gut, solange alle Enduser auf diese Daten nur über die Applikation1 zugreifen. Sobald diese Daten für andere Applikationen/Tools angewendet werden, greifen die Sicherheitsmechanismen der Applikation1 nicht mehr.

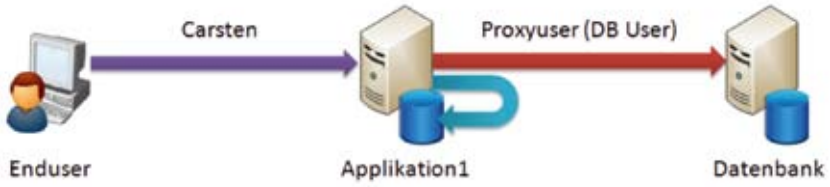

Abbildung 1: Beispiel für ein „Trusted Subsystem“-Modell

Beim „Impersonation“-Modell erfolgt die Autorisierung des Endbenutzers durch die Datenbank, bevor Zugriff auf die Daten gewährt wird (siehe Abbildung 2). Es gibt unterschiedliche Arten des „Impersonation“-Modells, die in der Oracle-Datenbankwelt möglich sind; die bekannteste ist die Client/Server-Art, bei der die Datenbank sowohl Authentifizierung als auch Autorisierung übernimmt.

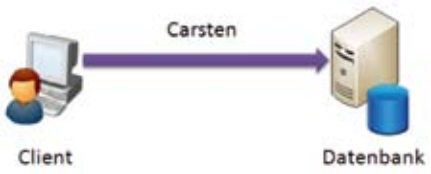

Abbildung 2: Beispiel für ein „Impersonation“-Modell

Das „Impersonation“-Modell unterstützt auch die Vorteile einer Three-Tier-Architektur und kann damit das Accounting und Auditing lösen. Ein Beispiel dafür ist das Oracle-Proxy-Authentication-Modell, zu dem die beiden Konzepte „Lightweight User Session“ und „Application User Proxy Authentication“ gehören (siehe Abbildung 3).

Viele Unternehmen setzen das Kerberos-Authentisierungsverfahren als unternehmensweiten Standard ein. Ihr Anliegen ist es, überall dort, wo es auch nur möglich ist, Kerberos als Authentifizierungsverfahren zu verwenden. Dazu hat Microsoft mit Windows Server 2003 die Funktionalitäten „Kerberos Constrained Delegation“ (A2D2) und „Protocol Transition“ (T2A4D) eingeführt, die nun von der Datenbank 11*g* R2 unterstützt werden.

Mit der „Kerberos Constrained Delegation“-Funktionalität befähigt man die Applikation1 (die die vorhandene Kerberos-Authentisierung nutzt), im Namen des Endbenutzers (im Bei-

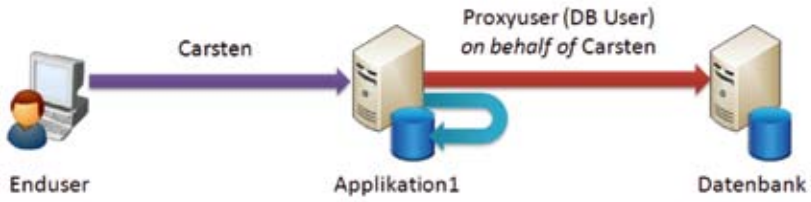

Abbildung 3: Beispiel für „Lightweight User Session” und „Oracle Proxy Authentication“

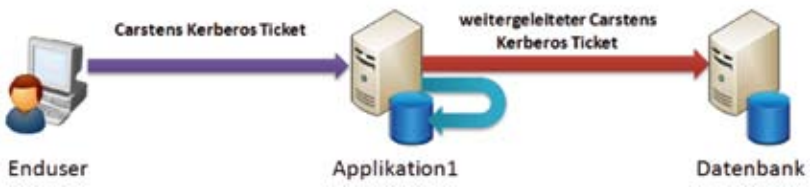

Abbildung 4: Beispiel für Kerberos Constrained Delegation

spiel „Carsten“) das Kerberos TGT-Ticket zu erstellen, um dieses dann an die Oracle-Datenbank weiterzugeben (siehe Abbildung 4). Die technischen Voraussetzungen dafür sind:

- Die Rechner, auf denen die Applikation1 und die Datenbank 11*g* R2 laufen, müssen mit dem Service Principal Name (SPN) bei dem MS Active Directory registriert sein und mit Kerberos Keytab-Files ausgestattet sein
- Die Datenbank 11*g* R2 verwendet den Kerberos Authentication-Adapter
- Das Kerberos-Ticket des Endusers („Carsten“) darf weitergeleitet werden (im MS Active Directory einzustellen)
- Die Applikation1 darf Kerberos-Tickets im Namen anderer erstellen (im MS Active Directory)

Die Funktionsweise für diese Authentisierungsdelegation ist folgende:

1. Carsten verbindet sich mit der Applikation1 und identifiziert sich mit seinem Kerberos-Service-Ticket, um den Dienst der Applikation1 in Anspruch zu nehmen.
2. Die Applikation1 muss auf die Oracle-Datenbank zugreifen, um die von Carsten angeforderten Daten zurückzuliefern. Demzufolge verlangt nun die Datenbank von der Applikation1, sich auszuweisen.
3. Die Applikation holt sich das TGT-Ticket von Carsten, lässt sich vom MS Active Directory das Service-Ticket für den Datenbankzugriff erstellen und greift daher mit den Benutzer-Informationen von Carsten auf die Datenbank zu.
4. Die Datenbank überprüft das Service-Ticket von Carsten, das die Applikation1 der Datenbank vorgelegt hat, und führt die Autorisierung durch.
5. Die Datenbank liefert die angeforderten Daten an die Applikation1 zurück, die diese dann an Carsten weitergibt.

Hiermit erreicht man Kerberos-Authentisierung auch dann, wenn kein direkter Verbindungskontakt zwischen dem Enduser und der Datenbank möglich ist. Die Vorteile sind:

- Das einheitliche und sichere Kerberos-Authentisierungsverfahren wird End-to-end benutzt. Somit ist eine starke Authentisierung durchgängig gegeben.
- Seitens des Endbenutzers ist keine erneute Anmeldung an der Datenbank notwendig.
- Herausforderungen wie Accounting und Auditing lassen sich einfach durch die Sicherheitsmechanismen der Datenbank zentralisiert lösen, womit dann die Anpassungen an den Applikationen entfallen.
- Des Weiteren greifen immer die Sicherheitsmechanismen der Datenbank, egal welche Komponente (Middleware, Applikation, DBA-Tool etc.) auf die Daten zugreifen will.

Es gibt aber auch Fälle, in denen die Anmeldung des Endusers an der Applikation1 nicht per Kerberos-Authentisierung erfolgt, da die Applikation Kerberos nicht unterstützt. Zudem kommt Kerberos vorwiegend im Intranet vor. Internet- und Extranet-Applikationen nutzen meist weiterhin Non-Kerberos-Authentisierungsverfahren.

Hierbei kommt jetzt die Funktionalität „Protocol Transition“ (T2A4D) zum Einsatz (siehe Abbildung 5). Mit dieser kann sich der Enduser an der Applikation1 mit Non-Kerberos-Authentifizierungsverfahren anmelden, die Applikation1 erstellt dann das Kerberos-Ticket in dessen Namen und greift auf die Datenbank zu.

Darüber hinaus unterstützt der Oracle Access Manager 11*g* R1 Kerberos-Authentisierung gerade für Web-Anwendungen. Somit kann der Oracle Access Manager die Endbenutzer automatisch an Web-Anwendungen mit ihren Desktop-Credentails mithilfe von Kerberos (Windows Native Authentication) authentisieren.

Weitere Informationen

- Advanced Security Option 11*g* R2 New Features: http://tinyurl.com/oracle-kerberos-11gr2
- Windows Native Authentication (Kerberos) mit dem Oracle Access Manager 11*g* R1: http://tinyurl.com/oam-kerberos-11gr1

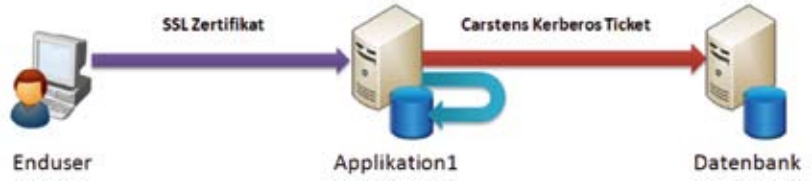

Abbildung 5: Beispiel für „Protocol Transition“

Kontakt:
Suvad Sahovic
suvad.sahovic@oracle.com
Carsten Mützlitz
carsten.muetzlitz@oracle.com